

**UNITED STATES DISTRICT COURT
DISTRICT OF NEBRASKA**

ANTONIA BIRD, individually, and on
behalf of all others similarly situated,

Plaintiff,

vs.

NELNET SERVICING, LLC,

Defendant.

Case No.

CLASS ACTION

**COMPLAINT FOR DAMAGES,
INJUNCTIVE AND EQUITABLE RELIEF
FOR:**

- 1. NEGLIGENCE;**
- 2. NEGLIGENCE *PER SE*;**
- 3. INVASION OF PRIVACY;**
- 4. BREACH OF CONFIDENCE;**
- 5. BREACH OF IMPLIED CONTRACT;**
- 6. BREACH OF THE IMPLIED COVENANT
OF GOOD FAITH AND FAIR DEALING;**
- 7. UNJUST ENRICHMENT.**

[JURY TRIAL DEMANDED]

Representative Plaintiff alleges as follows:

INTRODUCTION

1. Representative Plaintiff ANTONIA BIRD (“Bird” or “Representative Plaintiff”) brings this class action against Defendant NELNET SERVICING, LLC (“Nelnet” or “Defendant”) for its failure to properly secure and safeguard Representative Plaintiff’s and Class Members’ accounts and the personally identifiable information stored within Defendant’s information network, including, without limitation, full name, Social Security number, address, email address, and phone number. These types of information, *inter alia*, being hereafter referred to, collectively, as “personally identifiable information” or “PII”).¹ Defendant failed to properly secure and

¹ Personally identifiable information (“PII”) generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver’s license numbers, financial account numbers).

safeguard Representative Plaintiff's and Class Members' PII stored within Defendant's information network.

2. With this action, Representative Plaintiff seeks to hold Defendant responsible for the harms it caused and will continue to cause Representative Plaintiff and the countless other similarly situated persons in a security failure first identified by Defendant in July 2022, and occurring from June 2022 to July 22, 2022, by which cybercriminals were able to infiltrate Defendant's inadequately protected network servers and access Representative Plaintiff's and other customers' Social Security numbers and PII stored on Defendant's network servers.

3. Representative Plaintiff further seeks to hold Defendant responsible for not ensuring that the compromised PII and financial information was maintained in a manner consistent with industry and other relevant standards.

4. While Defendant claims to have detected unusual activity on its network as early as July 2022, it did not immediately report the security incident to Representative Plaintiff or Class Members. Indeed, Representative Plaintiff and Class Members were wholly unaware of the Data Breach until they received letter(s) from Defendant informing them of it. Defendant did not notify Class Members until August 26, 2022.

5. Defendant acquired, collected and stored Representative Plaintiff's and Class Members' PII and/or financial information in connection with Defendant's services.

6. Therefore, at all relevant times, Defendant knew, or should have known, that Representative Plaintiff and Class Members would use Defendant's networks to store and/or share sensitive data, including PII, because Defendant required that they provide this information to register and create an account with Defendant to use Defendant's services.

7. By obtaining, collecting, using, and deriving a benefit from Representative Plaintiff's and Class Members' PII and financial information, Defendant assumed legal and equitable duties to those individuals. These duties arise from state and federal statutes and regulations as well as common law principles.

8. Defendant disregarded the rights of Representative Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and

reasonable measures to ensure that Representative Plaintiff's and Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, failing to secure their accounts such that unauthorized individuals could not gain access to them, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Representative Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by further defrauding Representative Plaintiff and Class Members in the future. Representative Plaintiff and Class Members have a continuing interest in ensuring that their accounts are secure, and their information is and remains safe. As such, they are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

9. Jurisdiction is proper in this Court under 28 U.S.C. §1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of \$5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one other Class Member is a citizen of a state different from Defendant.

10. Supplemental jurisdiction to adjudicate issues pertaining to this state law is proper in this Court under 28 U.S.C. §1367.

11. Defendant Nelnet Servicing, LLC is a limited liability company organized in Nebraska with a principal place of business located at 121 S. 13th Street, Suite 100, Lincoln, Nebraska, 68508.

12. Defendant is a student loan servicing company. Defendant services loans across the United States, including to customers in this judicial district.

13. Defendant is the student loan servicer for Representative Plaintiff who resides in Oakland, California.

14. Venue is proper in this Court under 28 U.S.C. § 1391 because the events that gave rise to Representative Plaintiff's claims took place within this judicial district, and Defendant does business in this Judicial District.

15. A substantial portion of the underlying events and conduct occurred in this judicial district and the means of proof are largely located here.

PLAINTIFF

16. Representative Plaintiff is an adult individual and, at all relevant times herein, a resident of the State of California. Plaintiff's PII connected with her student loan and loan application which was and is in Defendant's possession and control, was accessed by unauthorized third parties.

17. In connection with the provision of loan services, Defendant collected PII and financial information from Representative Plaintiff. As a result, Representative Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

18. At all times herein relevant, Representative Plaintiff is and was a member of each of the Classes.

19. As required in order to purchase goods/services from Defendant, Representative Plaintiff provided Defendant with sensitive personal and financial information, including, without limitation, her name, Social Security number, address, email address, and phone number.

20. Representative Plaintiff's information was accessed by unauthorized third parties in light of Defendant's storage and/or sharing of Representative Plaintiff's PII and financial information. Representative Plaintiff's PII and financial information was, at all relevant times, within the possession and control of Defendant.

21. Due to Defendant's failure to adequately secure its system, Representative Plaintiff has already spent and will continue to spend time dealing with the consequences of this incident. This includes, without limitation, time spent verifying the legitimacy of transactions on her Nelnet account, exploring credit monitoring and identity theft insurance options, self-monitoring her

accounts, and seeking legal counsel regarding options for remedying and/or mitigating the effects of this incident. This time has been lost forever and cannot be recaptured.

22. Representative Plaintiff furthered suffered actual injury in the form of damages to and diminution in the value of Representative Plaintiff's PII—a form of intangible property that Representative Plaintiff entrusted to Defendant for the purpose of servicing and managing her student loan, which was compromised as a result of Defendant's failure to protect this information.

23. Representative Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of this incident and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cyber-criminals accessing and using sensitive PII and/or financial information.

24. Representative Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from Representative Plaintiff's PII and financial information, in combination with Representative Plaintiff's name, being placed in the hands of unauthorized third parties.

25. Representative Plaintiff has a continuing interest in ensuring that her account and the PII and financial information, which, upon information and belief, remains backed up and, thus, in Defendant's possession, is protected and safeguarded from future attacks or breaches.

DEFENDANT

26. Defendant Nelnet Servicing, LLC is a limited liability company formed in Nebraska with a principal place of business located at 121 S. 13th Street, Suite 100, Lincoln, Nebraska, 68508.

27. Defendant is a student loan servicing company operating throughout the country.

28. Defendant is the loan servicer for Representative Plaintiff located in Oakland, California.

29. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Representative Plaintiff. Representative Plaintiff will seek leave of court to amend

this Complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

CLASS ACTION ALLEGATIONS

30. Representative Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of Representative Plaintiff and the following class:

“All individuals within the United States of America whose PII and/or financial information was stored by Defendant and was exposed to unauthorized third parties as a result of the data breach discovered by Nelnet in July 2022 and occurring from June 2022 to July 22, 2022.”

31. Excluded from the Class are the following individuals and/or entities: (a) Defendant and Defendant’s parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; (b) all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; (c) any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and (d) all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

32. Representative Plaintiff reserves the right to request additional subclasses be added, as necessary, based on the types of PII and financial information that were compromised and/or the nature of certain Class Members’ relationship(s) to the Defendant. At present, collectively, Class Members include, *inter alia*, all persons within the United States whose Nelnet account and the PII and/or financial information thereon have been accessed by unauthorized third parties.

33. Representative Plaintiff reserves the right to amend the above definition in subsequent pleadings and/or motions for class certification.

34. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the proposed classes is easily ascertainable.

- a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff

Classes are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiff is informed and believes and, on that basis, alleges that the total number of Class Members is in the hundreds of thousands of individuals. Membership in the Classes will be determined by analysis of Defendant's records.

- b. Commonality: Representative Plaintiff and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:
- 1) Whether Defendant had a legal duty to Representative Plaintiff and the Classes to exercise due care in collecting, storing, using and/or safeguarding their PII;
 - 2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;
 - 3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;
 - 4) Whether Defendant's failure to implement adequate data security measures allowed a data breach to occur;
 - 5) Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
 - 6) Whether Defendant adequately, promptly, and accurately informed Representative Plaintiff and Class Members that their PII had been compromised;
 - 7) How and when Defendant actually learned of the cyber-intrusion;
 - 8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Representative Plaintiff and Class Members;
 - 9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the unauthorized access to occur;
 - 10) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Representative Plaintiff and Class Members;
 - 11) Whether Representative Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct;
 - 12) Whether Representative Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

- c. Typicality: Representative Plaintiff's claims are typical of the claims of the Plaintiff Classes. Representative Plaintiff and all members of the Plaintiff Classes sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein. The same event and conduct that gave rise to Representative Plaintiff's claims are identical to those that give rise to the claims of every Class Member because Representative Plaintiff and Class Members alike had their Stored Data compromised in the same way by the same conduct of Defendant. Representative Plaintiff and Class Members face identical threats resulting from the resetting of their hard drives and/or access by cyber-criminals to the Stored Data maintained thereon.
- d. Adequacy of Representation: Representative Plaintiff in this class action is an adequate representative of each of the Plaintiff Classes in that Representative Plaintiff has the same interest in the litigation of this case as the Class Members, is committed to vigorous prosecution of this case, and has retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Classes in their entirety. Representative Plaintiff anticipate no management difficulties in this litigation. Representative Plaintiff and its counsel will fairly and adequately protect the interests of all Class Members.
- e. Superiority of Class Action: The damages suffered by individual Class Members are significant but may be small relative to the enormous expense of individual litigation by each member. This makes or may make it impractical for members of the Plaintiff Classes to seek redress individually for the wrongful conduct alleged herein. Even if Class Members could afford such individual litigation, the court system could not. Should separate actions be brought or be required to be brought by each individual member of the Plaintiff Classes, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of other Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

35. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, such that it is impracticable to bring all Class Members before the Court.

36. This class action is also appropriate for certification because Defendant has acted and/or has refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Classes in their

entireties. Defendant's conduct challenged herein applies to and affects Class Members uniformly, and Representative Plaintiff's challenge to this conduct hinges on Defendant's conduct with respect to the Classes, and each of them, not on facts or law applicable only to the Representative Plaintiff.

37. Unless a Class-wide injunction is issued, Defendant's violations may continue, and Defendant may continue to act unlawfully as set forth in this Complaint.

COMMON FACTUAL ALLEGATIONS

The Cyberattack

38. One or more unauthorized third parties accessed Class Members' Nelnet accounts and the sensitive data stored therein including, but not limited to, full names, Social Security number, address, email address, and phone number.

39. Representative Plaintiff was among the individuals whose account was infiltrated and whose information was accessed.

40. Representative Plaintiff is not currently aware of the precise number of individuals similarly affected by Defendant's security lapses but believes it to be—at minimum—in the thousands. Representative Plaintiff bases this allegation on, *inter alia*, public statements by other Nelnet users reporting precisely the same problems as Representative Plaintiff during approximately the same time.

41. Representative Plaintiff was not aware of these security issues until learning that someone had gained access to her Nelnet account. To date, Defendant has not provided any explanation as to how or why someone was able to gain access to Representative Plaintiff's account and/or what steps it has and/or intends to take(n) to prevent further security failures.

42. Upon information and belief, the unauthorized third party cyber-criminals gained access to Representative Plaintiff's and Class Members' PII and financial information with the intent of engaging in misuse of the heretofore-described PII and financial information, including marketing and selling Representative Plaintiff's and Class Members' PII.

43. Defendant had and continues to have obligations created by reasonable industry standards, common law, state statutory law, and its own assurances and representations to keep Representative Plaintiff's and Class Members' PII confidential and to protect such PII from unauthorized access.

44. Representative Plaintiff and Class Members were required to provide their PII and financial information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

45. Despite this, Representative Plaintiff and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used, and what steps Defendant intends to take, if any, to secure Class Members' PII and financial information going forward. Representative Plaintiff and Class Members are left to speculate as to the full impact of this cyber-incident and how exactly Defendant intends to take so as to enhance its information security systems and/or monitoring capabilities so as to prevent further breaches.

46. Representative Plaintiff's and Class Members' PII and financial information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and financial information for targeted marketing without the approval of Representative Plaintiff and/or Class Members. Either way, unauthorized individuals can now easily access the PII and/or financial information of Representative Plaintiff and Class Members.

Defendant Collected/Stored Class Members' PII and Financial Information

47. Defendant acquired, collected, and stored and assured reasonable security over Representative Plaintiff's and Class Members' PII and financial information.

48. To use its services, Defendant required that Representative Plaintiff and Class Members provide them with their full name, address, email address, and Social Security number.

49. By obtaining, collecting, and storing Representative Plaintiff's and Class Members' PII and financial information, Defendant assumed legal and equitable duties and knew or should

have known that they were thereafter responsible for protecting Representative Plaintiff's and Class Members' PII and financial information from unauthorized disclosure.

50. Representative Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and financial information. Representative Plaintiff and Class Members relied on Defendant to keep their PII and financial information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

51. Defendant could have prevented the breach of Representative Plaintiff and Class Members' accounts by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Representative Plaintiff's and Class Members' PII and financial information.

52. Defendant's negligence in safeguarding Representative Plaintiff's and Class Members' PII and financial information is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending cyber-attacks in recent years.

53. Due to the high-profile nature of many recent cyber-attacks, Defendant was and/or certainly should have been on notice and aware of such attacks occurring and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendant is an e-commerce company and derives its revenue from operating an online marketplace.

54. Yet, despite the prevalence of public announcements of cyber-attacks and data security compromises, Defendant failed to take appropriate steps to protect Representative Plaintiff's and Class Members' PII and financial information from being compromised

Defendant Had an Obligation to Protect the Stolen Information

55. Defendant's failure to adequately secure Representative Plaintiff's and Class Members' sensitive data breaches duties it owed Representative Plaintiff and Class Members under statutory and common law. Representative Plaintiff and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep

it private and secure. Accordingly, Defendant also had an implied duty to safeguard their data, independent of any statute.

56. In addition to its obligations under federal and state laws, Defendant owed a duty to Representative Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII and financial information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Representative Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII and financial information of Representative Plaintiff and Class Members.

57. Defendant owed a duty to Representative Plaintiff and Class Members to design, maintain, and test its computer systems, servers and networks to ensure that the PII and financial information in its possession was adequately secured and protected.

58. Defendant owed a duty to Representative Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII and financial information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

59. Defendant owed a duty to Representative Plaintiff and Class Members to implement processes that would detect a breach on its data security systems in a timely manner.

60. Defendant owed a duty to Representative Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

61. Defendant owed a duty to Representative Plaintiff and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII and/or financial information from theft because such an inadequacy would be a material fact in their decision to entrust this PII and/or financial information to Defendant.

62. Defendant owed a duty of care to Representative Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

63. Defendant owed a duty to Representative Plaintiff and Class Members to encrypt and/or more reliably encrypt Representative Plaintiff's and Class Members' PII and financial information and monitor user behavior and activity in order to identify possible threats.

Value of the Relevant Sensitive Information

64. The ramifications of Defendant's failure to keep secure Representative Plaintiff's and Class Members' PII and financial information are long lasting and severe. Once PII and financial information is stolen, fraudulent use of that information and damage to victims may continue for years. Indeed, the PII and/or financial information of Representative Plaintiff and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII and/or financial information for that purpose. The fraudulent activity resulting from this may not come to light for years.

65. These criminal activities have and will result in devastating financial and personal losses to Representative Plaintiff and Class Members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiff and Class Members for the rest of their lives. They will need to remain constantly vigilant.

66. The FTC defines "identity theft" as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

67. Identity thieves can use PII and financial information, such as that of Representative Plaintiff and Class Members which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government

fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

68. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²

69. If cyber-criminals manage to access to personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Representative Plaintiff and Class Members.

70. Such security failures are easily preventable.³ As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."⁴ She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised"⁵

71. Most of the reported cyber-attacks are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.⁶

² Report to Congressional Requesters, GAO, at 29 (June 2007), available at: <http://www.gao.gov/new.items/d07737.pdf> (last accessed November 4, 2021).

³ Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

⁴ *Id.* at 17.

⁵ *Id.* at 28.

⁶ *Id.*

72. Here, Defendant knew of the importance of safeguarding PII and financial information and of the foreseeable consequences that would occur if Representative Plaintiff's and Class Members' PII and financial information was stolen, including the significant costs that would be placed on Representative Plaintiff and Class Members as a result of a successful attack. Defendant had the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Representative Plaintiff and Class Members. Defendant's failure to do so is, therefore, intentional, willful, reckless, and/or grossly negligent.

73. Defendant disregarded the rights of Representative Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Representative Plaintiff's and Class Members' PII and/or financial information; (iii) failing to take standard and reasonably available steps to secure representative Plaintiff and Class Members' accounts; (iv) concealing the existence and extent of the security failure for an unreasonable duration of time; and (v) failing to provide Representative Plaintiff and Class Members prompt and accurate notice.

FIRST CLAIM FOR RELIEF
Negligence
(On behalf of the Nationwide Class)

74. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

75. At all times herein relevant, Defendant owed Representative Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII and financial information and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the PII and financial information of Representative Plaintiff and Class Members in its computer systems and on its networks.

76. Among these duties, Defendant was expected:

- a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII and financial information in its possession;
- b. to protect Representative Plaintiff's and Class Members' PII and financial information using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;
- c. to implement processes to quickly detect any breaches and to timely act on warnings about cyber-attacks; and
- d. to promptly notify Representative Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII and financial information.

77. Defendant knew the PII and financial information was private and confidential. Representative Plaintiff and Class Members were foreseeable and probable victims of these inadequate security practices. As such, Defendant owed a duty of care not to subject Representative Plaintiff and Class Members to an unreasonable risk of harm.

78. Defendant knew or should have known of the risks inherent in collecting and storing PII and financial information, the vulnerabilities of its data security systems, and the importance of adequate security. Defendant knew about numerous, well-publicized cyber-attacks.

79. Defendant knew or should have known that its data systems and networks did not adequately safeguard Representative Plaintiff's and Class Members' accounts and PII/financial information.

80. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PII and financial information that Representative Plaintiff and Class Members had entrusted to it.

81. Defendant breached its duties to Representative Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII and financial information of Representative Plaintiff and Class Members.

82. Because Defendant knew that a breach of its systems could damage millions of individuals, including Representative Plaintiff and Class Members, Defendant had a duty to adequately protect those data systems and the PII and financial information contained thereon.

83. Representative Plaintiff's and Class Members' willingness to entrust Defendant with their PII and financial information was predicated on the understanding that Defendant would

take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the PII and financial information they stored on them from attack. Thus, Defendant had a special relationship with Representative Plaintiff and Class Members.

84. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Representative Plaintiff's and Class Members' PII and financial information and promptly notify them of any security failures. These "independent duties" are untethered to any contract between Defendant and Representative Plaintiff and/or the remaining Class Members.

85. Defendant breached its general duty of care to Representative Plaintiff and Class Members in, but not necessarily limited to, the following ways:

- a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII and financial information of Representative Plaintiff and Class Members;
- b. by failing to timely and accurately disclose that Representative Plaintiff's and Class Members' PII and financial information had been improperly acquired or accessed;
- c. by failing to adequately protect and safeguard the PII and financial information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII and financial information;
- d. by failing to provide adequate supervision and oversight of the PII and financial information with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII and financial information of Representative Plaintiff and Class Members, misuse the PII and intentionally disclose it to others without consent.
- e. by failing to adequately train its employees to not store PII and financial information longer than absolutely necessary;
- f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiff's and the Class Members' PII and financial information;
- g. by failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and
- h. by failing to encrypt Representative Plaintiff's and Class Members' PII and financial information and monitor user behavior and activity in order to identify possible threats.

86. Defendant's willful failure to abide by these duties was wrongful, reckless and grossly negligent in light of the foreseeable risks and known threats.

87. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Representative Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

88. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII and financial information to Representative Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PII and financial information.

89. Defendant breached its duty to notify Representative Plaintiff and Class Members of the unauthorized access by failing to notify Representative Plaintiff and Class Members of any security failures and then by failing and continuing to fail to provide Representative Plaintiff and Class Members sufficient information regarding attacks. To date, Defendant has not provided sufficient information to Representative Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Representative Plaintiff and Class Members.

90. Further, through its failure to provide timely and clear notification to Representative Plaintiff and Class Members, Defendant prevented Representative Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII and financial information.

91. There is a close causal connection between Defendant's failure to implement security measures to protect the accounts, PII, and financial information of Representative Plaintiff and Class Members and the harm suffered, or risk of imminent harm suffered by Representative Plaintiff and Class Members. Representative Plaintiff's and Class Members' PII and financial information was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII and financial information by adopting, implementing, and maintaining appropriate security measures.

92. Defendant's wrongful actions, inactions, and omissions constituted (and continues to constitute) common law negligence.

93. The damages Representative Plaintiff and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

94. Additionally, 15 U.S.C. §45 (FTC Act, Section 5) prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII and financial information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

95. Defendant violated 15 U.S.C. §45 by failing to use reasonable measures to protect PII and financial information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and financial information it obtained and stored and the foreseeable consequences of the immense damages that would result to Representative Plaintiff and Class Members.

96. As a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and financial information is used; (iii) the compromise, publication and/or theft of their PII and financial information; (iv) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud and/or unauthorized use of their PII and financial information; (v) lost opportunity costs associated with effort expended and the loss of productivity; (vi) addressing and attempting to mitigate actual and future consequences, including, but not limited to, efforts spent researching ways to prevent, detect, contest and/or recover from embarrassment and identity theft; (vii) the continued risk to their PII and financial information, which may remain in Defendant's possession and be the subject of further unauthorized disclosures so long as Defendant fails to undertake adequate measures to protect Representative Plaintiff's and Class Members' PII and financial information; and (viii) future costs (e.g., time, effort, money) that may/will be

expended to prevent, detect, contest and/or repair the harm(s) attendant to the compromise of Representative Plaintiff's and Class Members' PII and financial information.

97. As a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

98. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII and financial information, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and financial information in its continued possession.

SECOND CLAIM FOR RELIEF
Negligence *Per se*
(On behalf of the Nationwide Class)

99. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

100. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

101. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards described herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiffs and Class Members.

102. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

103. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

104. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class Members.

105. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Defendant's goods and services they received.

106. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

THIRD CLAIM FOR RELIEF
Invasion of Privacy
(On behalf of the Nationwide Class)

107. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

108. Representative Plaintiff and Class Members had a legitimate expectation of privacy to its PII and financial information and were entitled to the protection of this information against disclosure to unauthorized third parties.

109. Defendant owed a duty to Representative Plaintiff and Class Members to keep their PII and financial information confidential.

110. Defendant failed to protect and released to unknown and unauthorized third parties the PII and financial information of Representative Plaintiff and Class Members.

111. Defendant allowed unauthorized and unknown third parties access to and examination of the PII and financial information of Representative Plaintiff and Class Members, by way of Defendant's failure to protect the PII and financial information.

112. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII and financial information of Representative Plaintiff and Class Members is highly offensive to a reasonable person.

113. The unauthorized intrusion was into a place or thing which was private and is entitled to be private. Representative Plaintiff and Class Members disclosed their PII and financial information to Defendant as part of obtaining services from Defendants, but privately with an intention that the PII and financial information would be kept confidential and would be protected from unauthorized disclosure. Representative Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without its authorization.

114. The Data Breach constitutes an intentional interference with Representative Plaintiff's and Class Members' interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

115. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

116. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Representative Plaintiff and Class Members.

117. As a proximate result of the above acts and omissions of Defendants, the PII and financial information of Representative Plaintiff and Class Members was disclosed to third parties without authorization, causing Representative Plaintiff and Class Members to suffer damages.

118. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Representative Plaintiff and Class Members in that the PII and financial information maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Representative Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Representative Plaintiff and/or Class Members.

FOURTH CLAIM FOR RELIEF
Breach of Confidence
(On behalf of the Nationwide Class)

119. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

120. At all times during Representative Plaintiff's and Class Members' interactions with Defendants, Defendant were fully aware of the confidential nature of the PII and financial information that Representative Plaintiff and Class Members provided to them.

121. As alleged herein and above, Defendant's relationship with Representative Plaintiff and the Classes was governed by promises and expectations that Representative Plaintiff and Class Members' PII and financial information would be collected, stored, and protected in confidence,

and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

122. Representative Plaintiff and Class Members provided their respective PII and financial information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII and financial information to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

123. Representative Plaintiff and Class Members also provided their PII and financial information to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect their PII and financial information from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting its networks and data systems.

124. Defendant voluntarily received, in confidence, Representative Plaintiff's and Class Members' PII and financial information with the understanding that the PII and financial information would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by the public or any unauthorized third parties.

125. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, not following best information security practices to secure Representative Plaintiff's and Class Members' PII and financial information, Representative Plaintiff's and Class Members' PII and financial information was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized third parties beyond Representative Plaintiff's and Class Members' confidence, and without its express permission.

126. As a direct and proximate cause of Defendant's actions and/or omissions, Representative Plaintiff and Class Members have suffered damages, as alleged herein.

127. But for Defendant's failure to maintain and protect Representative Plaintiff's and Class Members' PII and financial information in violation of the parties' understanding of

confidence, its PII and financial information would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized third parties. The Data Breach was the direct and legal cause of the misuse of Representative Plaintiff's and Class Members' PII and financial information, as well as the resulting damages.

128. The injury and harm Representative Plaintiff and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendant's unauthorized misuse of Representative Plaintiff's and Class Members' PII and financial information. Defendant knew its data systems and protocols for accepting and securing Representative Plaintiff's and Class Members' PII and financial information had security and other vulnerabilities that placed Representative Plaintiff's and Class Members' PII and financial information in jeopardy.

129. As a direct and proximate result of Defendant's breaches of confidence, Representative Plaintiff and Class Members have suffered and will suffer injury, as alleged herein, including, but not limited to, (a) actual identity theft; (b) the compromise, publication, and/or theft of its PII and financial information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of its PII and financial information; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to its PII and financial information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Class Members' PII and financial information in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Representative Plaintiff and Class Members; (g) the diminished value of Representative Plaintiff's and Class Members' PII and financial information; and (h) the diminished value of Defendant's services for which Representative Plaintiff and Class Members paid and received.

FIFTH CLAIM FOR RELIEF
Breach of Implied Contract
(On behalf of the Nationwide Class)

130. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

131. Through its course of conduct, Defendant, Representative Plaintiff and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Representative Plaintiff's and Class Members' PII and financial information.

132. Defendant required Representative Plaintiff and Class Members to provide and entrust their PII and financial information, including full names, birthdates and prescription information and/or other financial information, as a condition of obtaining Defendant's services.

133. Defendant solicited and invited Representative Plaintiff and Class Members to provide their PII and financial information as part of Defendant's regular business practices. Representative Plaintiff and Class Members accepted Defendant's offers and provided their PII and financial information to Defendants.

134. As a condition of being direct customers/patients/employees of Defendants, Representative Plaintiff and Class Members provided and entrusted their PII and financial information to Defendants. In so doing, Representative Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Representative Plaintiff and Class Members if its data had been breached and compromised or stolen.

135. A meeting of the minds occurred when Representative Plaintiff and Class Members agreed to, and did, provide its PII and financial information to Defendants, in exchange for, amongst other things, the protection of its PII and financial information.

136. Representative Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

137. Defendant breached the implied contracts it made with Representative Plaintiff and Class Members by failing to safeguard and protect its PII and financial information and by failing

to provide timely and accurate notice to them that their PII and financial information was compromised as a result of the Data Breach.

138. As a direct and proximate result of Defendant's above-described breach of implied contract, Representative Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

SIXTH CLAIM FOR RELIEF
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Nationwide Class)

139. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

140. Every contract in the State of Illinois has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

141. Representative Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendants.

142. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII and financial information, failing to timely and accurately disclose the Data Breach to Representative Plaintiff and Class Members and continued acceptance of PII and financial information and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

143. Defendant acted in bad faith and/or with malicious motive in denying Representative Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

**SEVENTH CLAIM FOR RELIEF
Unjust Enrichment
(On behalf of the Nationwide Class)**

144. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

145. By its wrongful acts and omissions described herein, Defendant has obtained a benefit by unduly taking advantage of Representative Plaintiff and Class Members.

146. Defendants, prior to and at the time Representative Plaintiff and Class Members entrusted their PII and financial information to Defendant for the purpose of obtaining loan services, caused Representative Plaintiff and Class Members to reasonably believe that Defendant would keep such PII and financial information secure.

147. Defendant was aware, or should have been aware, that reasonable patients and consumers would have wanted their PII and financial information kept secure and would not have contracted with Defendant, directly or indirectly, had they known that Defendant's information systems were sub-standard for that purpose.

148. Defendant were also aware that, if the substandard condition of and vulnerabilities in its information systems were disclosed, it would negatively affect Representative Plaintiff's and Class Members' decisions to seek services therefrom.

149. Defendant failed to disclose facts pertaining to its substandard information systems, defects and vulnerabilities therein before Representative Plaintiff and Class Members made its decisions to make purchases, engage in commerce therewith, and seek services or information. Instead, Defendant suppressed and concealed such information. By concealing and suppressing that information, Defendant denied Representative Plaintiff and Class Members the ability to make a rational and informed decision as to their loan servicers, and took undue advantage of Representative Plaintiff and Class Members.

150. Defendant was unjustly enriched at the expense of Representative Plaintiff and Class Members. Defendant received profits, benefits, and compensation, in part, at the expense of Representative Plaintiff and Class Members. By contrast, Representative Plaintiff and Class

Members did not receive the benefit of their bargain because they paid for loan services that did not satisfy the purposes for which they bought/sought them.

151. Since Defendant's profits, benefits, and other compensation were obtained by improper means, Defendant is not legally or equitably entitled to retain any of the benefits, compensation or profits it realized from these transactions.

152. Representative Plaintiff and Class Members seek an Order of this Court requiring Defendant to refund, disgorge, and pay as restitution any profits, benefits and other compensation obtained by Defendant from its wrongful conduct and/or the establishment of a constructive trust from which Representative Plaintiff and Class Members may seek restitution.

RELIEF SOUGHT

WHEREFORE, Representative Plaintiff, individually and on behalf and each member of the proposed National Class, respectfully requests that the Court enter judgment in favor of the Plaintiff Classes and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including appointment of Representative Plaintiff's counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Representative Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to Representative Plaintiff and Class Members;

4. For injunctive relief requested by Representative Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Representative Plaintiff and Class Members, including but not limited to an Order:

- a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - c. requiring Defendant to delete and purge the PII of Representative Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Representative Plaintiff and Class Members;
 - d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiff's and Class Members' PII;
 - e. requiring Defendant to engage independent third party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;
 - f. prohibiting Defendant from maintaining Representative Plaintiff's and Class Members' PII on a cloud-based database;
 - g. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
 - h. requiring Defendant to conduct regular database scanning and securing checks;
 - i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Representative Plaintiff and Class Members;
 - j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
 - k. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;
 - l. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.
- 5. For prejudgment interest on all amounts awarded, at the prevailing legal rate;
 - 6. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

7. For all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Representative Plaintiff, individually and on behalf of the Plaintiff Class(es) and/or Subclass(es), hereby demands a trial by jury for all issues triable by jury.

Dated: September 8, 2022

Respectfully submitted,

/s/ Cody Alexander Boloce
Cody Bolce, Esq.
California State Bar #322725
COLE & VAN NOTE
555 12th Street, Suite 1725
Oakland, CA 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: cab@colevannote.com

Attorneys for Representative Plaintiff Tri Thai
and the Plaintiff Class(es)